BINUS UNIVERSITY GRADUATE PROGRAM Master Program | Master of Computer Science

HYBRID CONSENSUS ALGORITHM UNTUK VALIDASI DOKUMEN PADA JARINGAN *BLOCKCHAIN* PRIVAT

Student

Shibron Arby Azizy
2502482992
shibron.azizy@binus.ac.id

Thesis Advisor

Dr. Aditya Kurniawan, S.Kom., MMSI., CND, CEHmaster
D3448

1 Introduction

Document validation is a fundamental process in government institutions to ensure the authenticity and integrity of official projects. In Indonesia, the Ministry of Public Works manages thousands of contract documents annually that must be validated to support compliance and prevent auditing errors. However, the current validation system remains centralized and manual, causing inefficiencies, increased operational costs, and potential security risks. Conventional approaches rely heavily on human-centric workflows that lack automation and transparency (Gandhi et al., 2023), while the use of physical copies creates significant overhead due to manual verification, paper storage, and auditing (Haveri et al., 2020). Even after lengthy and costly certification processes, final attested documents can still be forged digitally, highlighting the insecurity of traditional mechanisms (Aldwairi et al., 2023). To overcome these issues, this study proposes a private blockchain with a hybrid PoA–PoW consensus, combining fast validation with robust ledger security to ensure integrity and trust.

2 Previous Work

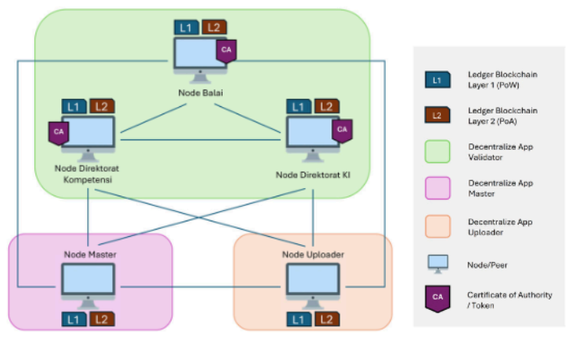
Several studies have explored blockchain for document validation using different approaches. Gandhi et al. (2023) proposed a public Ethereum-based architecture with strong transparency through smart contracts, but the high transaction cost (gas fee) makes it unsuitable for government settings. Similarly, Rana et al. (2023) applied a hybrid PoS–PoA consensus on Polygon MATIC for securing digital evidence, yet the reliance on public networks still introduces transaction fees that are less suitable for cost-sensitive institutions.

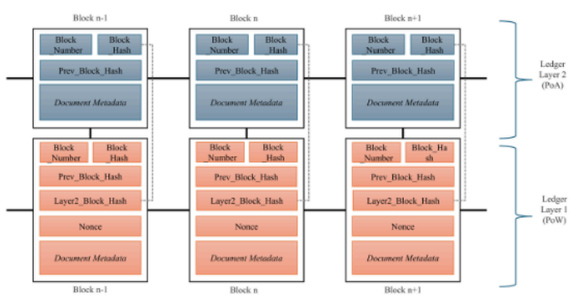
Other research emphasized private blockchain solutions. Pericàs-Gornals et al. (2022) designed a PoA-based system on the Ethereum Virtual Machine to validate COVID-19 certificates, ensuring privacy and immutability. However, the use of a single PoA consensus creates a single point of trust and increases risks of manipulation at validator nodes. Moreover, relying on the Rinkeby test network is unstable for government-scale systems due to its limited reliability

Cash and Bassiouni (2018) also explored a hybrid two-layer architecture combining PoW and PoA, showing that PoA enables efficient validation while PoW strengthens ledger integrity against tampering. Building on this idea, the present study proposes a custom private blockchain with hybrid PoA–PoW, where PoA on Layer 2 ensures fast document validation and PoW on Layer 1 enhances security. This design also integrates QR codes as digital proof and eliminates transaction fees, making it more suitable for government institutions that demand efficiency, integrity, and full infrastructure control.

3 Methodology

The private blockchain architecture consists of five nodes: three validators, one uploader, and one master, where each node maintains two ledgers. Layer 2 (PoA) enables fast validation and issuance of Certificate Authorities (CAs), while Layer 1 (PoW) secures the ledger against tampering. This hybrid design ensures both efficiency and strong security for government document validation.



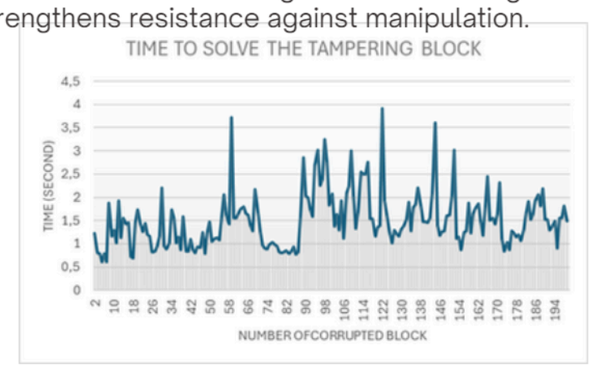


The ledger architecture is designed in two layers: Layer 2 (PoA) for document validation and Layer 1 (PoW) for securing the ledger. Both layers are interconnected through a single reference value (layer2_block_hash) stored in the PoW ledger, creating a strong linkage between them. This dual-layer design ensures that each transaction is represented in two different blocks, making the system more resilient against manipulation.

4 Results

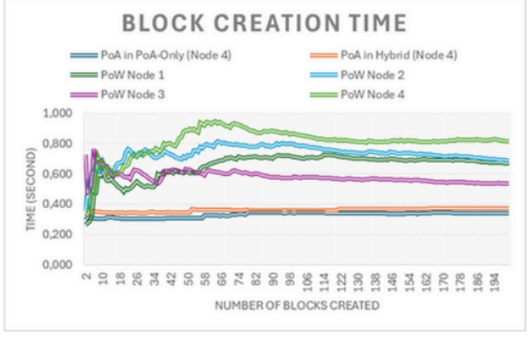
Security Test

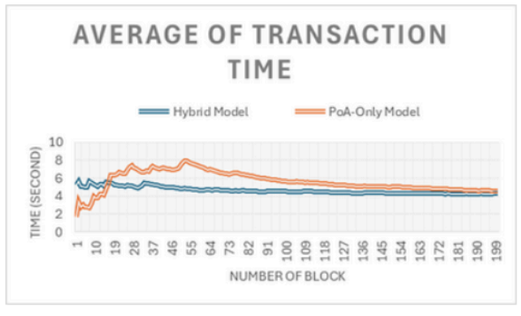
Security evaluation was conducted through **200 block tampering simulations,** where invalid or manipulated blocks were injected into the ledger. The system successfully detected and repaired all corrupted ledgers, with an **average recovery time of 1.50 seconds**. This proves that the dual-layer design with cross-referencing hashes significantly strengthens resistance against manipulation.

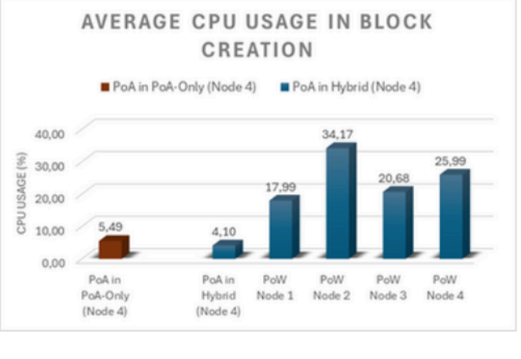


Performance Test

The hybrid PoA–PoW system demonstrated efficient performance across three aspects. Transaction time averaged 4.31 seconds, slightly faster than the PoA-only model (4.57 seconds), showing that adding PoW did not reduce validation efficiency. In the hybrid model, PoA block creation averaged 0.371 seconds, slightly higher than the PoA-only model (0.339 seconds) due to the overhead of initiating PoW mining. On the PoW layer, block creation averaged 0.677 seconds across four slave nodes, which is **slower** but reinforces ledger immutability through computational validation. Meanwhile, CPU usage during PoW mining increased almost 7× compared to PoA-only, but remained acceptable as the trade-off directly enhanced system security.







5 Conclusion

This study introduced a hybrid consensus model that combines PoA and PoW for secure and efficient document validation in private blockchain networks. By separating fast PoA-based validation from asynchronous PoW-based ledger verification, the system achieves both high performance and resilience. The hybrid model maintained a stable average transaction time of 4.31 seconds, with PoA and PoW block creation averaging 0.371 and 0.677 seconds respectively. In security tests, the system successfully recovered all 200 tampered ledgers within an average of 1.50 seconds, ensuring 100% restoration of ledger integrity. These results demonstrate that integrating PoW into a PoA-based system enhances security and robustness without sacrificing validation efficiency.

Future development can focus on improving efficiency and scalability, for example by grouping multiple documents within a single block to reduce storage usage and processing time. The system should also incorporate version control to track document revisions such as contract changes or addendums, thereby enhancing accountability in the validation process. In addition, further optimization of Proof of Work and large-scale testing with more nodes on physical machines are recommended to ensure stability and robustness under real operational conditions.

6 References

- Aldwairi, M., Badra, M., & Borghol, R. (2023). DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution. 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA), 652–657. https://doi.org/10.1109/BCCA58897.2023.10338908
- Cash, M., & Bassiouni, M. (2018). Two-Tier Permission-ed and Permission-Less Blockchain for Secure Data Sharing. 2018 IEEE International Conference on Smart Cloud (SmartCloud), 138–144. https://doi.org/10.1109/SmartCloud.2018.00031
- Gandhi, S., Kiwelekar, A., Netak, L., & Shahare, S. (2023). A blockchain-based data-driven trustworthy approval process system. International Journal of Information Management Data Insights, 3, 100162. https://doi.org/10.1016/j.jjimei.2023.100162
- Haveri, P., Rashmi, U. B., Narayan, D. G., Nagaratna, K., & Shivaraj, K. (2020). EduBlock: Securing Educational Documents using Blockchain Technology. 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 1–7. https://doi.org/10.1109/ICCCNT49239.2020.9225265
- Pericàs-Gornals, R., Mut-Puigserver, M., & Payeras-Capellà, M. M. (2022). Highly private blockchain-based management system for digital COVID-19 certificates. International Journal of Information Security, 21(5), 1069–1090. https://doi.org/10.1007/s10207-022-00598-3
- Rana, S. K., Rana, A. K., Rana, S. K., Sharma, V., Lilhore, U. K., Khalaf, O. I., & Galletta, A. (2023). Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain. IEEE Access, 11, 83289–83300. https://doi.org/10.1109/ACCESS.2023.3302771